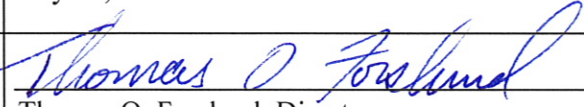




Thomas O. Forslund, Director

Governor Matthew H. Mead

<b>Policy Title:</b>	Information Access Control
<b>Policy Number:</b>	S-015
<b>Effective Date:</b>	July 15, 2013
<b>Approval:</b>	<div><div> Thomas O. Forslund, Director</div><div><u>7/15/13</u> Date</div></div>

**Purpose:**

To prevent and/or detect and correct undesired security incidents, this policy establishes parameters regarding user access to information and information systems. The confidentiality and integrity of information assets stored on systems managed by both Wyoming Department of Health (WDH) and its business associates requires assurance that authorized users have access to only specified information assets.

**Scope:**

This policy applies to all types of information in all formats (electronic, magnetic, paper or other) generated, used, or maintained by WDH within the scope of its business processes. All individuals who have been granted access to WDH information or information systems, including, but not limited to, full- and part-time employees, contractors, temporary workers, those employed by others to perform WDH work, and others granted access are covered by this policy and shall comply with this and associated policies, procedures, and guidelines.

**Policy:**

**1. General**

- a. WDH shall establish access controls to its information assets and systems. Only authorized users shall be granted access. Information users are limited to specific defined, documented, and approved systems and applications and levels of access rights.
- b. WDH shall apply the minimum necessary principle to determine role-based access privileges. This principle applies to all information held by WDH, confidential and non-confidential, including official personnel and supervisor working files.
  - i. Information shall be disclosed only to those persons who have a legitimate business need for the information.
  - ii. Reasonable efforts shall be made to limit the amount of information accessed to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
  - iii. Consistent with WDH Policy AS-004; Minimum Necessary Information, WDH divisions/programs/facilities shall identify functional categories of information necessary for classes of persons in their workforce to carry out their duties and any conditions appropriate to such access by using WDH Form F-026; Functional Categories.
  - iv. Assignment of workforce members to functional categories shall be documented using WDH Form F-028; Assignment of Functional Category.
- c. Access shall be granted based on paragraph 1.b. above. Access to WDH information shall be granted by the appropriate workforce (generally, WDH or its business associate) with primary responsibility for specified information assets. Requests for access approval shall be processed in a timely manner.

- d. Information users are required to sign a WDH Form F-002; Acknowledgment of Training as a condition of access approval. Regular acknowledgments shall be required for all information users.
- e. WDH's information assets shall be classified by levels of sensitivity, confidentiality, and risk associated with inappropriate disclosure.
- f. Information assets, whether paper or electronic, shall be protected through access controls. Access controls are intended to prevent improper disclosure, modification, deletion, or rendering data unavailable. Examples of access controls include locked file cabinets, secured building access (codes and ID badges), traditional system passwords, and other secure technologies.
- g. Access controls shall be applied consistently to information assets throughout their life cycle. Information assets are to be protected in a manner commensurate with their classification regardless of where they reside, the form they take, the technology used to maintain them, and the purpose(s) they serve.

## **2. Responsibilities**

- a. Information users shall be expected to apply the concepts of this policy to their day-to-day operations to achieve consistent information protection.
- b. WDH shall evaluate information users' roles on a regular basis to confirm the appropriateness of access levels. Program managers shall request change to access level privileges when user needs change.
- c. WDH shall maintain a list of workforce and business associates who have primary responsibility for WDH information assets and the domain of WDH information assets to which their authority extends.
- d. The WDH security officer shall monitor and log all significant security incidents related to information assets. The security officer shall establish monitoring, record collection, and reporting for security incidents.
- e. The WDH security officer shall develop and maintain an exception process to address extraordinary, case-by-case access requests that are beyond the scope of the established role-based categories.

## **3. Identification**

- a. All users approved to access system and information assets shall be properly identified.
- b. Approved workforce members shall be informed of WDH security policies, regulations, and user responsibilities associated with access to information assets and systems. Users shall be informed of:
  - i. Acknowledgments required to access information assets and systems;
  - ii. Responsibilities regarding use of access controls such as user IDs, passwords, keys and locks;
  - iii. Responsibilities to report known or suspected security incidents; and
  - iv. WDH's intent to monitor its computer systems for compliance with this policy.

## **4. Authentication**

- a. Upon notification of access approval, system administrators shall ensure a unique user identification is assigned to the authorized information user.
- b. Information systems shall authenticate all users, where applicable. Unauthorized users shall be denied access.
- c. User identification and authentication may not be required for access to those information assets with the lowest level of security classification.
- d. Temporary, manual authentication procedures shall be developed for contingency use when a technical system or technical security feature is unavailable for use.

**5. Revoking Access Privileges**

- a. The following circumstances require supervisors to timely request appropriate modification and/or revocation of user access privileges to information assets and systems:
  - i. Modification of access privileges when employees separate or transfer by appointment, assignment, or job rotation;
  - ii. Revocation of access privileges during employee absence when deemed appropriate; and
  - iii. Revocation of access privileges upon employee separation. This includes revoking access privileges to systems, restricted access zones, and facilities, and retrieving all security related items issued to the individual such as badges, keys, documents, etc.
- b. Where possible, automatic revocation of access privileges shall occur after 30 days of inactivity.

**6. Contracting**

For all contracts with external organizations that affect information assets, information services, or information technology equipment, divisions/programs/facilities are responsible for implementing business associate agreements that require such organizations to comply with applicable requirements of the Security Rule.

**Contacts:**

De Anna Greene, CIPP/US, CIPP/G, CIPP/IT, WDH Privacy/Compliance Officer, (307) 777-8664  
Tate Nuckols, JD, WDH Security Officer, (307) 777-2438

**Forms:**

F-026; Functional Categories  
F-028; Assignment of Functional Category Acknowledgement

**Policies:**

AS-004; Minimum Necessary Information

**References:**

45 CFR §§ 164.306-312

**Training:**